

## AUTOMATIC CONFIGURATION OF CLIENT TERMINAL IN PUBLIC HOT SPOT

## RELATED APPLICATION

5        This application claims the benefit of U.S. Provisional Application No. 60/454,551, filed March 14, 2003, and incorporated herein by reference.

## 1. Field of the invention

10      The invention provides an apparatus and a method for in which a client terminal is automatically configured for access to a communications network, and in particular, a WLAN system automatically configures an IEEE 802.1x client on the wireless user device through the client web browser and an ActiveX control or a functionally equivalent plug-in. The IEEE 802.1x client configured in this manner is then able access with the WLAN system using the appropriate authentication parameters.

15

## 2. Description of Related Art

15      The context of the present invention is the family of wireless local area networks or (WLAN) employing the IEEE 802.1x architecture having an access point (AP) that provides access for mobile devices and to other networks, such as hard wired local area and global networks, such as the Internet. Advancements in WLAN technology have resulted in the publicly accessible wireless communication at rest stops, cafes, libraries and similar public facilities ("hot spots"). Presently, public WLANs offer mobile communication device users access to a private data network, such as a corporate intranet, or a public data network such as the Internet, peer to peer communication and live wireless TV broadcasting. The relatively low cost to implement and operate a public WLAN, as well as the available high bandwidth (usually in excess of 10 Megabits/second) makes the public WLAN an ideal access mechanism, through which, mobile wireless communications device users can exchange packets with an external entity. However as will be discussed below, such open deployment may compromise security unless adequate means for identification and authentication exists.

20      When a user attempts to access service within a public WLAN coverage area, the WLAN first authenticates and authorizes user access, prior to granting network access. After authentication, the public WLAN opens a secure data channel to the mobile communications device to protect the privacy of data passing between the WLAN and the device. Presently, many manufacturers of WLAN equipment have adopted the IEEE 802.1x protocol for

deployed equipment. Hence, the predominant authentication mechanism for WLANs utilize this protocol, which can be difficult to reconfigure for the average user.

The IEEE 802.1x protocol was designed with private LAN access as its usage model. Hence, the IEEE 802.1x protocol does not provide certain features that would improve the 5 security in a public WLAN environment. For example IEEE 802.1x clients normally require complex configurations as by way of example, authentication methods, authentication server domain names, user names and passwords, that are complex and therefore can be difficult for users to understand. If a user attempts to access a new public hot spot, one or more of the parameters required for access user's device may require reconfiguration. In addition to 10 gaining access, the 802.1x client may have to establish an account with the new public hot spot. As such the prior art does not establish such accounts in a transparent and seamless fashion, so as to make hot spot access cumbersome and impractical.

In the current web browser based authentication method, a mobile terminal 15 communicates with a local or a remote authentication server, using a web browser operating with the Hyper Text Transfer Protocol Secured Sockets (HTTPS) protocol to insure that anyone on the path between the mobile terminal and the authentication server cannot trespass upon or steal confidential user information. However, the only information the authentication server has related to the mobile terminal is its IP address. A practical solution to 20 reconfiguring a client requires that it operate within the standards established by the 802.1x protocol. However, the inventors have discovered a means that modifies the behavior within the restrictions of the protocol, by filtering traffic, such that the user is allowed access to the network rather than experiencing a block, which would prevent the further automatic reconfiguration to achieve authentication.

## SUMMARY OF THE INVENTION

25 The method of the present invention provides for automatic configuration of a client terminal to access a communications network. In particular, the method according to the invention utilizes IEEE 802.1x, the adopted protocol for secure IEEE 802.11 wireless access, for authentication. Furthermore, a web browser together with an ActiveX control or plug-in for natural user interactions may include, among other things, the creation of user accounts, 30 the selection of which accounts to use, and the acceptance of access terms. As the result of the user interactions, IEEE 802.1x client parameters are automatically configured according to user choices, and permit a secure authentication based on the IEEE 802.1x protocol.

The invention herein provides a method for automatically configuring an IEEE 802.1x client terminal to provide limited access in a WLAN environment comprising the steps of the WLAN filtering traffic associated with the limited access and thereby redirecting the client terminal HTTP request to a designated web server, whereby the web server responds to the client terminal by requesting information required to establish an authorized communication. Thereafter, the client terminal provides the web server information required to establish an authorized communication. In the course of the communication the web server indicates to the client terminal information corresponding to such parameters as transmission rates, user account requirements, authentication method selection information, new account creation procedures, user terms and conditions which are all typically required to establish an authorized communication. The client terminal user responds accordingly with web server access rate information, web server user account creation information, user access authentication method selection information, and user acceptance of the offered service required to establish an authorized communication.

The method further comprises the step whereby the web server responds to the client terminal utilizing a plug-in control such as an ActiveX control to communicate information required to establish an authorized communication. The client terminal thereafter reconfigures its terminal to establish secure access to the network.

The present invention also includes one or more apparatus that cooperate in providing a secure communications session between a client terminal 140<sub>n</sub> and a WLAN. The client terminal requests access to the WLAN through an access means. The WLAN processes the request sending it to a packet filter that redirects the client to a designated web server. The web server responds by providing provider list web pages, which are processed by means where the user inputs its selection and sends the client terminal access information. The web server responds by sending an ActiveX Control to configure the client terminal utilizing a means for activating, in response to the information received from the client terminal, a software module that reconfigures the client terminal and establish an authorized communication. Thereafter the client access means permits authenticated access to pass through the WLAN. The WLAN provides a means for authenticating the reconfigured client terminal and allows access to the WLAN in response to the authentication using appropriate parameters associated with a configuration arrangement selected by a user.

#### BRIEF DESCRIPTION OF THE DRAWINGS

The invention is best understood from the following detailed description when read in

connection with the accompanying drawing. The various features of the drawings are not specified exhaustively. On the contrary, the various features may be arbitrarily expanded or reduced for clarity. Included in the drawing are the following figures:

5 FIG. 1 is a block diagram of a communications system for practicing the method of the present principles for authenticating a mobile wireless communications device.

FIG. 2 is a flow diagram of the inventive method of establishing authentication when the IEEE 802.1x protocol.

10

FIG. 3 is a block diagram of an apparatus for implementing the present invention.

#### DETAILED DESCRIPTION OF THE INVENTION

In the figures to be discussed, the circuits and associated blocks and arrows represent

15 functions of the process according to the present invention, which may be implemented as electrical circuits and associated wires or data busses that transport electrical signals. Alternatively, one or more associated arrows may represent communication (e.g., data flow) between software routines, particularly when the present method or apparatus of the present invention is implemented as a digital process.

20 When a user operating a terminal incorporating the IEEE 802.1x protocol ("client terminal" or simply "IEEE 802.1x client") attempts to access a public WLAN at a hot spot, the IEEE 802.1x client terminal would begin the authentication process according to its current machine configuration. Often the user terminal is not configured for access at a particular hot spot (e.g. it could be configured for office use, or the user may not have an account that permits access to a particular hot spot). The user opens its browser and attempts to access the network. With a modified behavior of the WLAN access point in accordance with the present invention, the user requests are redirected to a local web server, also referred to as an HTTP server. The web server in response sends the terminal various requirements that must be fulfilled to establish access to the network. If the user fulfills the requirements the 25 web server authorizes access.

30

The typical sequence proceeds with the web server providing a greeting page that contains a list of service providers that the user may desire to use for authentication and charging. Selecting one of the providers would activate the ActiveX control/plug-in on the

user's terminal. When the required parameters are specified by the terminal the user will be successfully authenticated by the service provider. Using these parameters, the ActiveX control/plug-in configures the IEEE 802.1x client and restarts the authentication process. The user is thereafter successfully authenticated and the WLAN AP fully opens access to the user.

5 If the user does not have any existing accounts that would permit authentication, the greeting page also allows the user to create a new account. Upon creation of the account, the ActiveX control/plug-in is activated to allow the reconfiguration of the terminal to proceed.

In accordance with FIG. 1, one or more mobile terminals represented by 140<sub>1</sub> through 140<sub>n</sub> communicate over a wireless medium 124 through an access point (AP) through 130<sub>n</sub>,

10 local computer 120, which may be utilized as the HTTP server 120 (FIG. 2), in association with firewalls 122 and one or more virtual operators 150<sub>1-n</sub>, such as authentication server 150<sub>n</sub>. Communication from terminals 140<sub>1-n</sub> typically require accessing a secured data base or other resources, utilizing the Internet 110 and associated communication paths 154 and 152 that require a high degree of security from unauthorized entities, such as would be hackers.

15 As further illustrated in FIG. 1, the WLAN architecture encompasses several components and services that interact to provide station mobility transparent to the higher layers of a network stack. The AP stations such as access points 130<sub>1-n</sub> and mobile terminals 140<sub>1-n</sub> as the components connect to the wireless medium and typically contain the functionality of the IEEE 802.1x protocols, that being MAC (Medium Access Control) 134<sub>1-n</sub>, 20 and corresponding PHY (Physical Layer) (unshown), and a connection 127 to the wireless media. Communication functions and protocols are implemented in the hardware and software of a wireless modem or a network access or interface card. This invention proposes a method for implementing a means in the communication stream, such that an access point 130<sub>n</sub> improves the authentication of a terminal device in a WLAN environment, and remain within 25 the compatibility requirements of a IEEE 802.1x WLAN MAC layers for downlink traffic (i.e. from the an authentication server to the mobile terminal such as a laptop) as it may participate in the authentication of one or more wireless mobile devices 140<sub>1-n</sub>, a local server 120 and a virtual operator such as the server 150.

30 In accordance with the principles of the present invention, an access 160 enables each mobile terminals 140<sub>1-n</sub>, to securely access a WLAN 115 by authenticating both the mobile terminal itself, as well as its communication stream in accordance with the IEEE 802.1x protocol or other optional protocol as the terminal 140<sub>n</sub> may choose. The manner in which the access 160 enables such secure access can best be understood by reference to FIG. 2, which

depicts the sequence of interactions that occurs among a mobile wireless communication device, say mobile terminal 140<sub>n</sub>, the public WLAN 115, and a HTTP server 120<sub>n</sub>. When configured with the IEEE 802.1 x protocols, the access point 130<sub>n</sub> of FIG. 1 maintains a controlled port and an un-controlled port, through which the access point exchanges

5 information with the mobile terminal 140<sub>n</sub>. The controlled port maintained by the access point 130<sub>n</sub> serves as the entryway for non-authentication information, such as data traffic, to pass through the access point 130<sub>n</sub> between the WLAN 124 and the mobile terminals 140<sub>n</sub>. Ordinarily, the access point 130<sub>n</sub> keeps the respective controlled port closed in accordance with the IEEE 802.1x protocol, until authentication of the mobile wireless communications

10 device. The access points 130<sub>n</sub> always maintains the respective uncontrolled port open to permit the mobile terminals 140<sub>n</sub> to exchange authentication data with the local server 150<sub>n</sub>.

The access point includes an 802.1X engine 325, which is a module that implements the IEEE 802.1X protocol with the determining means necessary to carry out the steps of the present invention. The WLAN 115 system must maintain proper state information for the

15 system to function properly. Such state information will be provided by the access point 130<sub>n</sub> 802.1x engine, which is used by, among other things, the packet filtering function 330 and the HTTP server 120. With reference to FIG. 2, a further embodiment of the present invention is the utilization of the access point 130<sub>n</sub> to create several operational states. Following a Response-Identity EAP packet 220 a state 1x\_progress 340 indicates that the mobile terminal

20 140<sub>n</sub> is an IEEE 802.1x client and the 802.1x authentication process is ongoing. Such means to select from one or more available security protocols is well known by those skilled in the art of programming and engineering in a WLAN environment. The 802.1X engine 325 is therefore responsible for client detection and providing the client capability information to other modules of the system. In addition it also implements RADIUS client functionality to

25 convert EAP messages to RADIUS messages, forwarding such messages in the form of a radius access request 230 and responding to radius access reject messages 240. The packet filter module 330 is responsible for filtering packets based on the criteria set by other modules.

In the event, a EAP-Response-Identity packet 220 results in a state 1x\_failure 350

30 because, as by way of example, the client is not properly configured, the client would be redirected to the local HTTP server 120 to attempt a reconfiguration of the client. More particularly, FIG. 2 illustrates an embodiment of the method of the present invention wherein the access point 130<sub>n</sub> detects that the mobile terminal 140<sub>n</sub> is not an authenticated IEEE

802.1x client, and a redirect client 335 moves the process to thereby configure through an IP packet filter module 330 and move the process to the HTTP server 120 via a web request redirect 345. Alternatively, mobile terminal 140<sub>n</sub> may send a direct web access request 355, which is redirected by the packet filter module 330 to the HTTP server 120. When the HTTP 5 server 120 receives a web redirect request 345 it responds by presenting the mobile terminal 140<sub>n</sub> with information 360, such as a provider list web page, specifically related to the browser based authentication.

In the case where the access point 130<sub>n</sub> detects that the terminal device is an IEEE 802.1x client, it permits normal IEEE 802.1x protocol communication exchanges to proceed 10 through the access point 130<sub>n</sub> and sets up appropriate IP packet filtering through IP filter module 330 and requisite state information for the HTTP server 120 to control the mobile terminal 140<sub>n</sub> user access during and after the IEEE 802.1x based authentication process.

The invention herein provides a method for automatically configuring a IEEE 802.1x client terminal to provide limited access in a WLAN 115 comprising the steps of an access 15 point 130<sub>n</sub> filtering traffic 330 associated with the limited access and thereby redirecting via a web request redirect 345 the client terminal 140<sub>n</sub> to the designated HTTP web server 120, whereby the web server responds to the client terminal 140<sub>n</sub> by sending information 360 required to establish an authorized communication. Thereafter the client terminal 140<sub>n</sub> provides the web server information 365 such as the provider selected, to establish an 20 authorized communication. In the course of the communication the web server 120 indicates to the client terminal 140<sub>n</sub> information corresponding to such parameters as transmission rates, user account creation information, authentication method selection information, new account 25 creation procedures, access user terms and conditions of acceptance, all typically required to establish an authorized communication. The client terminal 140<sub>n</sub> user responds 365, accordingly communicating web server 120 access rate information, web server user account creation information, user access authentication method selection information, and user access terms and conditions of acceptance information required to establish an authorized communication. The HTTP server 120 invokes 370 a plug-in such as an ActiveX control plug to assist the terminal 140<sub>n</sub> in reconfiguring 375 the terminal 140<sub>n</sub>.

30 In referring to FIG. 3, the present invention also includes an apparatus for providing a secure communications session between a client terminal 140<sub>n</sub> and a WLAN 115. The client terminal 140<sub>n</sub> requests through means 445 access to the WLAN 115 through the access point 130<sub>n</sub> receiver 405, which processes the request through means 418 and sends the request to a

packet filter 420 that redirects the client to a designated web server via transmit means 424. The web server responds to the client terminal 140<sub>n</sub> by providing provider list web pages, which are processed by means 448 where the user inputs its selection through a means 448 and sends the client terminal 140<sub>n</sub> access information through transmit means 470. The web

5 server responds by sending an ActiveX Control to configure the client terminal 140<sub>n</sub> utilizing a means 465 for activating, in response to the information received from the client terminal, a software module that reconfigures the client terminal and establish an authorized communication. Thereafter the client access means 480 permits authenticated access to pass through the WLAN 115. The access point 130<sub>n</sub> provides a means for authenticating the

10 reconfigured client terminal and allows access to the WLAN in response to the authentication using appropriate parameters associated with a configuration arrangement selected by a user.

The access point 130<sub>n</sub> for providing a secure communications session between the client terminal a 140<sub>n</sub> and the WLAN 115, comprises a means for receiving an access request 418 from the terminal 140<sub>n</sub>; a means for redirecting the access request 420,422 to a local web

15 server.

In response to the access request the terminal 140<sub>n</sub>, information required to establish terminal 140<sub>n</sub> access to the WLAN 115; the terminal 140<sub>n</sub> is provided web page options. The client terminal select through means 448 the desired configuration.

In response to the information received from the client terminal 140<sub>n</sub>, the web server

20 sends a configuration and the client terminal processes the configuration utilizing a means for activating 465, comprising a software module that reconfigures the client terminal 140<sub>n</sub> for authentication, using appropriate parameters associated with a configuration arrangement selected by a user; and a means for authenticating 425 the reconfigured client terminal 140<sub>n</sub>, and allowing access to the WLAN 115 in response to the authentication.

25 It is to be understood that the form of this invention as shown is merely a preferred embodiment. Various changes may be made in the function and arrangement of parts; equivalent means may be substituted for those illustrated and described; and certain features may be used independently from others without departing from the spirit and scope of the invention as defined in the following claims.